E-mail content monitoring system

Publication number: CN1350247 (A)
Publication date: 2002-05-22
Inventor(s): LI JIANHUA [CN]; WANG MINGZHENG [CN]; SU BO [CN]
Applicant(s): UNIV SHANGHAI JIAOTONG [CN]
Classification:
- international: ***G06F17/00; H04L29/06;*** **G06F17/00; H04L29/06;** (IPC1-7): G06F17/00; H04L29/06
- European:
Application number: CN20011039010 20011203
Priority number(s): CN20011039010 20011203

Abstract of **CN 1350247 (A)**

The monitoring system of mail contents comprising original mail services, which is characterized by that it also comprises a monitoring system server, and said server comprises a main program module and contents filter function module, garbage mail preventing module, information recording module, rule management module and administration auditing module which can be respectively called by said main program. Said administration auditing module can respectively make reel-time control of rule management module, information recording module and main program module. Said invention possesses obvious effect for preventing garbage mail, pornographic mail, attack mail and mail bomb, and its success rate is above 85%. Besides, it does not affect the delivery effect of original mail server.

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 17/00
H04L 29/06

[12]发明专利申请公开说明书

[21]申请号 01139010.7

[43]公开日 2002年5月22日

[11]公开号 CN 1350247A

[22]申请日 2001.12.3 [21]申请号 01139010.7

[71]申请人 上海交通大学
地址 200030 上海市华山路1954号
[72]发明人 李建华 王明政 苏 波

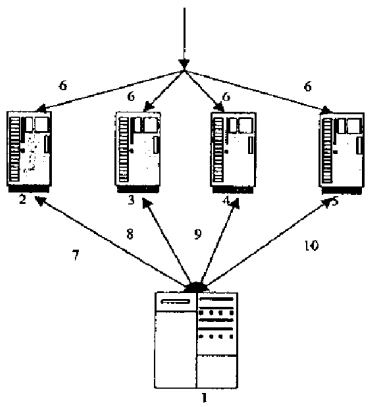
[74]专利代理机构 中原信达知识产权代理有限责任公司
代理人 文 琦

权利要求书2页 说明书7页 附图页数1页

[54]发明名称 针对邮件内容的监管系统

[57]摘要

一种针对邮件内容的监管系统，包括原邮件服务器2、3、4、5，特点是，还有一监管系统服务器1，而且，该服务器1含有一主程序模块11和分别受 其调用的内容过滤功能模块12、防垃圾邮件模块13、信息记录模块14和规 则管理模块16以及管理审计模块15，该管理审计模块分别实时地控制该规 则管理模块16、信息记录模块14和主程序模块11。本发明的效果是显著的，对于预防垃圾邮件、邮件炸弹起到了明显的作用，成功率在85%以上；对于 过滤内容具有色情、攻击性以及反动言论等的邮件有非常好的效果，90%的 此类信件都被系统识别并拦截；另外，对于原邮件服务器的邮件投递效率没有任何不良影响。



ISSN1008-4274

01.12.10

权 利 要 求 书

1、一种针对邮件内容的监管系统，包括原邮件服务器（2、3、4、5），其特征在于，还有一与该等原邮件服务器（2、3、4、5）分别以网路（7、8、9、10）成双向连接的监管系统服务器（1），而且，该服务器（1）含有一主程序模块（11）和分别受其调用的内容过滤功能模块（12）、防垃圾邮件模块（13）、信息记录模块（14）和规则管理模块（16）以及管理审计模块（15），该管理审计模块（15）分别实时地控制该规则管理模块（16）、信息记录模块（14）和主程序模块（11）。

2、根据权利要求 1 所述的针对邮件内容的监管系统，其特征在于，所说的原邮件服务器（2、3、4、5）与终端用户的邮件投递以简单邮件传输协议连接。

3、根据权利要求 1 所述的针对邮件内容的监管系统，其特征在于，所说的主程序模块（11）具有完成相关邮件信息记录、管理员操作日志记录写入功能。

4、根据权利要求 1 所述的针对邮件内容的监管系统，其特征在于，所说的内容过滤功能模块（12）系根据过滤规则完成对邮件正文和附件的文字检查。

5、根据权利要求 1 所述的针对邮件内容的监管系统，其特征在于，所说的防垃圾邮件模块（13），其实现基于 IP 地址的邮件炸弹防护、包括对发信频率和数量的统计、判断与处理；邮件字段“发

送者”、“接收者”、“抄送”、“标题”、“来源地址”、以及发信人真实性判断的检查。

6、根据权利要求 1 所述的针对邮件内容的监管系统，其特征在于，所说的信息记录模块（13），其包括对删除邮件的摘要信息记录，拦截邮件的完整信息记录以及管理人员的操作日志记录。

7、根据权利要求 1 所述的针对邮件内容的监管系统，其特征在于，所说的规则管理模块（16）是对监管系统使用的所有规则统一管理。

8、根据权利要求 1 所述的针对邮件内容的监管系统，其特征在于，所说的管理审计模块（15），其系提供管理界面，使管理人员可实时控制监管系统，对拦截邮件作人工查看，对安全策略、过滤规则、系统参数作设置与动态调整。

说　明　书

针对邮件内容的监管系统

技术领域

本发明涉及一种网络信息安全监管系统，具体地说，是一种关于对网络邮件内容的监管系统。

背景技术

邮件安全问题包括两个方面：作为网络服务系统的安全问题和邮件内容的安全问题。因此，邮件安全系统的开发也相应从两个方面来着手工作：邮件系统安全和邮件内容安全。邮件内容安全目前主要通过垃圾邮件检测、内容过滤等技术来实现。

垃圾邮件（SPAM）一般包括 UBE（非请求大宗电子邮件）以及 UCE（非请求商业电子邮件）。此类邮件发件率高，数量大，且占用了网络资源，影响邮件服务器性能，妨碍了用户对正常电子邮件的接受。目前，垃圾邮件防护技术主要是检测邮件的各字段，及时发现并过滤垃圾邮件。一般按照关键字对邮件的发送者、接收者、抄送、标题等字段进行简单的过滤。

为了进一步对邮件做过滤，仅仅用简单的垃圾邮件防护技术是不充分的。还需要对邮件内容——即邮件正文及附件进行文字检查，防止诸如色情、攻击性以及反动言论通过邮件进行大面积传播。基于邮件内容的检测防护技术

还相对缺乏。主要是对邮件内容进行全文匹配，判断是否出现特点的关键字，过滤技术比较简单。

由于对图片等其它多媒体形式文件尚没有有效的检查过滤方式，所以，内容过滤主要限于对邮件文字的过滤。

邮件的投递过程中主要使用 SMTP（简单邮件传输协议）协议和 POP3（邮件投递协议）协议。其中，客户端向邮件服务器发送邮件时使用 SMTP 协议，客户端从邮件服务器接收邮件使用 POP3 协议。从邮件服务器的角度来看，垃圾邮件与内容具有危害性的邮件都是外界通过 SMTP 协议投递到邮件服务器的用户邮箱。因而，对外部通过 SMTP 协议投递到本地邮件服务器的邮件进行过滤，就达到了保护本地邮件用户不受垃圾邮件、反动邮件等的危害的目的。

由于以前针对邮件内容的检测技术的相对不成熟，所以，目前各种类型的邮件系统普遍缺乏基于邮件内容的邮件检测防护机制。

发明内容

本发明的目的在于提供一种针对邮件内容的监管系统，其基于邮件内容检测的邮件过滤机制，结合系统自动处理与管理员人工操作两种方式，最终实现对邮件的有效过滤。

本发明是这样实现的：

监管系统与原邮件服务器是在不同的服务器上分离运行的，即本发明包

括：原邮件服务器，其对外接收使用 SMTP 协议投递来的邮件，特点是，在把邮件送交到相应邮件用户信箱之前，提取邮件信息，送交监管系统所在的服务器，等待监管系统的反馈指令。监管系统对邮件信息进行分析，判断邮件的危险级别，然后向邮件系统所在服务器发送反馈指令，决定邮件系统是否将该邮件送交到邮件用户信箱。这样，就在保证了邮件服务器正常运行的同时，实现了对邮件的过滤。其中，为了使邮件服务器能够具有提取邮件信息并送交监管系统的功能，需要对原邮件服务器作适当改造，这种改造不会影响邮件服务器邮件投递过程中的其它步骤。

概括来说，本发明的针对邮件内容的监管系统，其包括原邮件服务器，其特点是，还有一与该原邮件服务器分别以网路成双向连接的监管系统服务器，而且，该服务器含有一主程序模块和分别受其调用的内容过滤功能模块、防垃圾邮件模块、信息记录模块和规则管理模块以及管理审计模块，该管理审计模块分别实时地控制该规则管理模块、信息记录模块和主程序模块，所说的邮件服务器与终端用户的邮件投递以 SMTP 简单邮件传输协议连接。

本发明的效果是显著的，其在中国上海东方网的邮件服务器上应用后，对于预防垃圾邮件、邮件炸弹起到了明显的作用，成功率在 85%以上。对于过滤内容具有色情、攻击性以及反动言论等的邮件有非常好的效果。90%的此类信件都被系统识别并拦截。对于东方网原邮件服务器的邮件投递效率没有任何不良影响。

附图说明

图 1 是本发明系统实施应用示意图。

图 2 是本发明监管系统服务器内部模块示意图。

具体实施方式

根据图 1 和图 2 给出本发明的实施例。

本实施例的邮件内容安全监管系统与东方网的邮件服务器协同运行，如图 1 所示。

其包括邮件内容安全监管系统服务器 1，它与东方网原邮件服务器 2、3、4、5 成双向联结。

箭头 6 表示外部向东方网通过 SMTP 协议投递信件。

箭头 7、8、9、10 从邮件服务器 2、3、4、5 到监管系统端方向表示邮件服务器 2、3、4、5 将提取的邮件信息送交监管系统所在的服务器 1；箭头 7、8、9、10 从监管系统端到邮件服务器 2、3、4、5 方向表示监管系统的反馈指令。

邮件服务器 2、3、4、5：将每封邮件的发信人 IP、邮件数据信息发送给监管系统服务器 1，根据监管系统服务器 1 返回信息对邮件进行删除、拦截、正常放行等处理。

监管系统服务器 1：提供防邮件炸弹、防垃圾邮件转发服务以及邮件正文及附件的文字过滤服务，根据用户设置的安全策略及过滤规则，对邮件进行分析处理，并将结果通过命令形式反馈给邮件服务器 2、3、4、5。

对监管系统服务器 1 的内部模块如图 2 所示，其中：

规则管理模块 16：对监管系统使用的所有规则统一管理，供主程序模块调用。

主程序模块 11：完成对防垃圾邮件、内容过滤功能、过滤规则的调用，完成相关邮件信息记录、管理员操作日志记录写入功能。

内容过滤功能模块 12：根据过滤规则完成对邮件正文、附件的文字检查。

防垃圾邮件模块 13：实现基于 IP 地址的邮件炸弹防护，包括发信频率和数量进行统计、判断与处理；邮件字段“发送者”、“接收者”、“抄送”、“标题”、“来源地址”，以及发信人真实性判断的检查。

信息记录模块 14：包括对删除邮件的摘要信息记录，拦截邮件的完整信息记录以及管理人员操作日志记录。

管理审计模块 15：提供管理界面，使管理员可以对监管系统作实时控制；对拦截邮件作人工察看；对安全策略、过滤规则、系统参数作设置与动态调整。

箭头 17、18、19、20 表示：主程序模块 11 对其它模块的统一调用控制。

箭头 21、22、23 表示：管理审计模块 15 对其它模块的实时控制。其中箭头 23 是对信息记录模块 14 中的拦截邮件作人工察看处理；箭头 21 是对主程序模块 1 中的主程序的实时控制，设置系统基本参数；箭头 22 是对规则管理模块 1 中的过滤规则的维护。

在本实施例中，监管系统的运行流程如下：

1. 系统初始化设置。监管系统首先调入相关参数、安全策略和过滤规则库等，为过滤作初始化准备。
2. 监听端口，等待邮件服务器送交的邮件信息。
3. 对邮件服务器送交的邮件信息，启动主程序，进行过滤。
4. 主程序按照过滤规则对邮件的信息进行综合检查，包括对邮件的字段“发送者”、“接收者”、“抄送”、“标题”、“来源地址”的检查；对邮件正文以及文本形式的附件的内容检查；发信人真实性判断，发信频率、数量的动态统计判断等。综合检查后，主程序给出邮件危险级别。
5. 监管系统根据预定的安全策略，按照邮件危险级别来决定对该邮件的相应处理方式。系统对危险级别较高的邮件直接删除，同时在数据库中记录该邮件的摘要信息留作记录；对级别较低的邮件暂时拦截，将该邮件的完整信息记录在数据库中留待管理员人工处理；对普通级别的邮件直接放行。各个级别间的界限由安全策略决定，可以动态调整。其中，对邮件的删除、拦截、放行是在邮件服务器端实现的。这样，就完成了对邮件内容过滤的全过程。
6. 在监管系统运行过程中，系统允许管理员通过管理界面对监管系统作实时控制，对安全策略、过滤规则、系统参数作动态调整。
7. 监管系统可以随时启动、停止，在监管系统停止时原邮件服务器就恢复为不具有过滤功能的普通邮件服务器。监管系统在运行时，对原邮

件服务器的邮件投递速度效率的影响可以忽略，因而，不会对原邮件服务器的邮件投递造成不良影响。

说　明　书　附　图

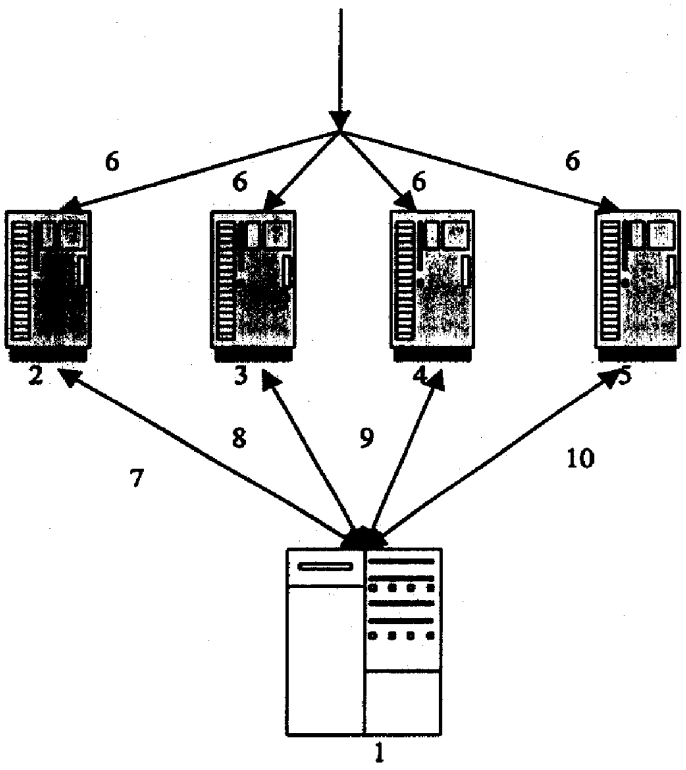


图 1

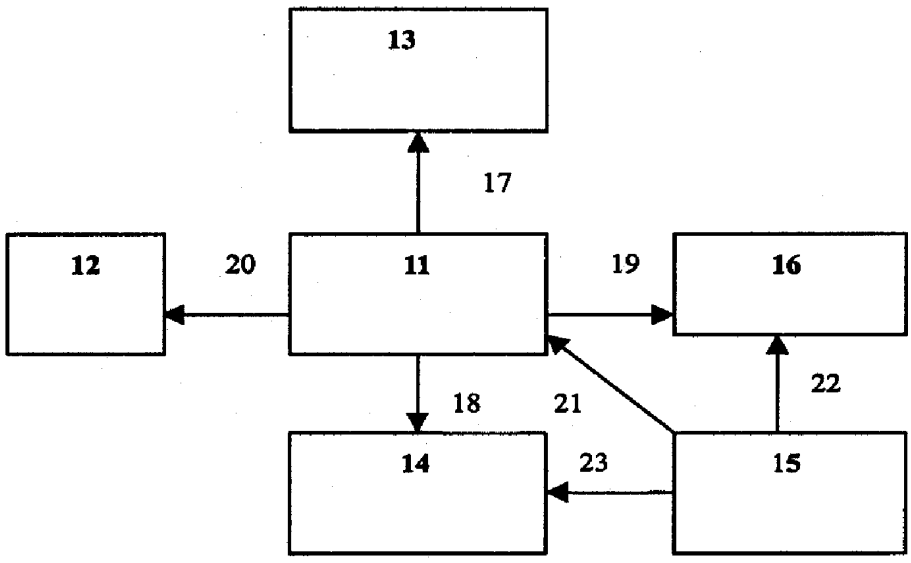


图 2